

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General



Bureau of Industry and Security

***FY 2009 FISMA Assessment of
BIS IT Infrastructure (BI)
(BIS002)***

Final Inspection Report No. OSE-19574/September 2009

Office of Audit and Evaluation





UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

September 30, 2009

MEMORANDUM FOR: Daniel O. Hill
Acting Under Secretary for Industry and Security and
Deputy Under Secretary for Industry and Security

FROM: Allen Crawley
Assistant Inspector General
for Systems Acquisition and IT Security

SUBJECT: Bureau of Industry and Security
FY 2009 FISMA Assessment of BIS IT Infrastructure (BI)
(BIS002)
Final Inspection Report No. OSE-19574

This report presents the results of our Federal Information Security Management Act (FISMA) review of BIS' continuous monitoring of security controls as part of the certification and accreditation (C&A) process for the BIS IT Infrastructure (BIS002).

We found that BIS' continuous monitoring for BIS002 did not meet Department and FISMA continuous monitoring requirements. We found that continuous monitoring has not been conducted since accreditation of the system in FY 2006 and that significant C&A deficiencies identified by the OIG in FY 2006 following C&A have not been corrected. In addition, OIG's own assessment of selected security controls found numerous vulnerabilities requiring remediation. Our findings are of particular concern because BIS has categorized BI as a [REDACTED]

In its response to our draft report, BIS did not dispute our findings but did not specifically indicate whether it agreed with our recommendations. After receiving BIS's response, I spoke with BIS' acting chief information officer, who stated that BIS agreed with our findings and recommendations. BIS' response is included in its entirety as appendix C.

We request that you provide us with an action plan describing the actions you have taken or plan to take in response to our recommendations within 60 calendar days of the date of this report. A plan of action and milestones should be used to communicate the plan as required by FISMA.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-1855.

Attachment

cc: Suzanne Hilding, chief information officer, U.S. Department of Commerce
Eddie Donnell, acting chief information officer, BIS
Raushi Conrad, director, System and Security Operations, BIS

Listing of Abbreviated Terms and Acronyms

BI	BIS IT Infrastructure System
BIS	Bureau of Industry and Security
C&A	Certification and Accreditation
CIO	Chief Information Officer
[REDACTED]	[REDACTED]
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
[REDACTED]	[REDACTED]
IP	Internet Protocol
IT	Information Technology
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
[REDACTED]	[REDACTED]
SID	System Identifier
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Synopsis of Findings

- Continuous monitoring has not been conducted since the FY 2006 accreditation.
- Significant certification and accreditation deficiencies previously identified by OIG have not been corrected.
- OIG assessments found vulnerabilities requiring remediation.

Conclusion

Since the BIS IT Infrastructure system (BI) was authorized to operate in June 2006, BIS has not followed the Department's IT security policy and NIST requirements for securing this [REDACTED] system. BIS has not conducted control assessments, assessed the impact of configuration changes on the system, reported and corrected known vulnerabilities, and addressed significant deficiencies identified in a previous OIG evaluation conducted in FY 2006. As a result, the system owner has not provided the authorizing official with assurance that the required controls are adequately protecting the system and its information. Thus, BIS should not have reported to OMB and the Department that annual assessments of security controls were conducted or that the system was certified and accredited.

Summary of BIS Response

In its response to our draft report, BIS did not dispute our findings but did not specifically indicate whether it agreed with our recommendations.

BIS explained that it will produce an action plan to address our recommendations, and its FY 2010 President's Request will provide the resources needed to replace the system with a more secure infrastructure.

BIS' response is included in its entirety as appendix C of this report.

OIG Comments

After receiving BIS' response, OIG's assistant inspector general for systems acquisition and IT security spoke with BIS' acting chief information officer, who stated that BIS agreed with our findings and recommendations.

Introduction

BI provides headquarters and 11 field offices with services that include e-mail, office automation, correspondence and assignment tracking, secure remote file access, export licensing storage, and management of BIS legal documents. At headquarters, BIS relies on the Department's network infrastructure to provide IT security services such as firewall protection, content monitoring and filtering, and network-based intrusion detection. BIS' deputy under secretary for Industry and Security authorized BI to operate on June 26, 2006.

Because BI processes [REDACTED] data, BIS has categorized it as a [REDACTED] system, which means that a security breach could be expected to have a [REDACTED] effect on organizational operations, organizational assets, or individuals.

Findings and Recommendations

1. Continuous Monitoring Has Not Been Conducted Since the FY 2006 Accreditation

Background: NIST SP 800-37 emphasizes that continuous monitoring is a critical aspect of certification and accreditation (C&A) and requires four essential activities: (1) configuration management and control of information system components, (2) security impact analyses of changes to the system, (3) assessment of security controls, and (4) status reporting.

- Configuration management and security impact analyses have not been conducted.
 - Because system changes have not been managed, BIS system administrators could not explain, and the system security plan did not describe [REDACTED]
 - The system inventory BIS provided does not accurately represent the current operational system (see table 1).
 - BIS told us that 31 system components have been removed from the accreditation boundary.
 - Twenty-two are still listed on the system inventory despite having been retired and disconnected from the network. Our assessments confirmed they are no longer connected.
 - Our assessments found nine of these system components to be connected, active, and accessible. BIS staff was not aware these components were still active and was unsure of the operational impact of removing them.
 - [REDACTED]
 - Although significant changes have been made to the system, the security plan has not been updated since BI was last certified and accredited in 2006.
 - Effective security protection requires a clear understanding of changes to servers, workstations, laptops, and application software components.
 - Comprehensive implementation of security controls requires an accurate inventory of system components and applications.
 - Security plans are required to be updated at least annually or when a significant system change is made.
 - BIS did not conduct analyses to determine the security impact of system changes.
 - Analysis is required to determine if changes to the system affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls.
 - Security impact analysis is an essential risk management activity, [REDACTED].
- Continuous assessment of security controls has not been done.
 - BIS reported to the Department Chief Information Officer (CIO) that annual assessments of security controls were conducted in FY 2007 and FY 2008. However, BIS could not provide OIG with the assessment procedures used to

assess controls, assessment result artifacts, vulnerabilities identified by the assessments, or any other evidence to support its claim that annual assessments were conducted.

- Vulnerability scanning was conducted by the Department, but BIS could not provide any evidence that the scanning results were analyzed or corrective actions were taken.
- NIST emphasizes the importance of continuously assessing security controls to ensure they are operating as intended and protecting the information system appropriately.
- BIS management and staff have not used the plan of action and milestones (POA&M) to manage known vulnerabilities.
 - No POA&MS were created to address vulnerabilities since 2006.
 - BIS also failed to add vulnerabilities known prior to C&A in 2006 to the POA&M. These vulnerabilities include [REDACTED]
 - Some of the vulnerabilities BIS has not documented in a POA&M or corrected can be remediated by administrative actions requiring minimal effort, such as the following:
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - BIS asserted that it does not use the POA&M to record vulnerabilities that are fixed within 90 days of discovery or for which management accepts the associated risk. However, BIS could not provide any evidence of vulnerabilities that were remediated or for which risks were accepted.
 - POA&Ms are required to track and manage system weaknesses and inform the authorizing official of corrective actions needed, resources required, responsible individuals, and scheduled completion dates.

Recommendations

BIS should

- 1.1 implement a change management methodology to approve system changes, conduct security impact analyses of changes to the system, and update the system security plan;
- 1.2 develop and conduct continuous monitoring assessments of selected NIST 800-53 security controls using NIST SP800-53A as required by OMB; and
- 1.3 ensure that all known vulnerabilities are documented in the system's POA&M or that the authorizing official is informed of and accepts the associated risk.

2. Significant Certification and Accreditation Deficiencies Previously Identified by OIG Have Not Been Corrected

BI was certified and accredited June 26, 2006. OIG evaluated the C&A package as part of its FY 2006 Federal Information Security Management Act of 2002 (FISMA) evaluation and presented the following findings to BIS on March 7, 2007.

- OIG's evaluation found that certification testing did not adequately assess the required security controls and that the authorizing official lacked information needed to make a credible, risk-based decision on whether to authorize system operation. As a result, in our FY 2006 FISMA report to OMB, we reported this system as **not** certified and accredited. We presented the following significant deficiencies requiring management attention:
 - The system security plan did not clearly describe the system architecture, component inventory, and implementation of security controls for a [REDACTED] system.
 - Secure configuration settings for IT products were not established, implemented, or assessed.
 - Security control assessments were inadequate.
 - Assessment results were not provided.
 - Procedures to assess security controls were not applied to all system components.
 - Controls were assessed by examining policy and interviewing staff rather than examining or testing the controls' implementation on system components.
 - Vulnerability scanning did not assess all system components at [REDACTED] and [REDACTED].
 - Penetration testing [REDACTED] was not performed.
 - Contingency plan testing was not supported by evidence.
- In a memorandum dated March 19, 2007, BIS' IT security officer informed OIG management that BIS had planned to reaccredit this system to address these deficiencies, as well as significant changes made since the FY 2006 accreditation, by December 2007. BIS' then-CIO, in an e-mail to OIG management on January 8, 2009, stated that effort was not completed because of budget constraints.
- Since accrediting the system in FY 2006, BIS has not followed the Department IT security policy and NIST requirements for maintaining and monitoring system security controls.
- The system owner has not provided the authorizing official with assurance that the required controls are adequately protecting the system and its information.
- BI's C&A expired on June 25, 2009. BIS is planning to migrate the information and functionality of BI to a new system. This migration, however, may not be completed until 2011 and is dependent on the development, deployment, and accreditation of the new system. Currently, BIS has no formal plan to reaccredit the BI system.

Recommendations

BIS should

- 2.1 report to the Department that BI is **not** certified and accredited; and
- 2.2 manage the security risks of operating BI until it is retired by assessing the effectiveness of security controls, determining the remaining risks, developing and implementing a plan of action and milestones to mitigate those risks, and reporting regularly to the authorizing official and BIS' acting CIO concerning the status of milestones.

Table 1. System Components Not Properly Managed or Documented

Component Name	IP Address	OIG Comments
[REDACTED]	[REDACTED]	<p>These components have been retired, but are still listed in the system inventory.</p>
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	<p>These components have been retired, but are still listed in the system inventory.</p>
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	<p>These components have been retired, but are still listed in the system inventory.</p>
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	<p>Although BI management claimed that these components had been retired from the system, they are still active and accessible from the network.</p>
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]

*All component IP addresses and names (including those labeled "Unknown") are excerpts from the system inventory.

Table 2. Vulnerabilities Identified by OIG Assessments

Security Control	NIST SP 800-53 Requirement	Vulnerability
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 2. Vulnerabilities Identified by OIG Assessments

Security Control	NIST SP 800-53 Requirement	Vulnerability
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]

Table 2. Vulnerabilities Identified by OIG Assessments

Security Control	NIST SP 800-53 Requirement	Vulnerability
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 2. Vulnerabilities Identified by OIG Assessments

Security Control	NIST SP 800-53 Requirement	Vulnerability
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 3. Vulnerabilities Identified by OIG Using the Nessus Vulnerability Scanner

Host Name	Port	Vulnerability Description
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 3. Vulnerabilities Identified by OIG Using the Nessus Vulnerability Scanner

Host Name	Port	Vulnerability Description
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]

Table 3. Vulnerabilities Identified by OIG Using the Nessus Vulnerability Scanner

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Appendix A: Objectives, Scope, and Methodology

To meet the FY 2009 Federal Information Security Management Act (FISMA) reporting requirements, we evaluated BIS' continuous monitoring activities for the BIS IT Infrastructure System (BI) since the system's accreditation in FY 2006.

Continuous monitoring is a critical postaccreditation aspect of the security C&A process. Effective continuous monitoring programs require four activities:

- configuration management and control of information system components
- security impact analyses of changes to the system
- assessment of security controls
- status reporting

NIST SP 800-53 notes that an effective continuous monitoring program results in ongoing updates to the system security plan, the security assessment report, and the plan of action and milestones (POA&M)—the three principle documents in the security accreditation package. Through continuous monitoring, the authorizing official is kept apprised of the security posture of the information system.

The objectives of our evaluation were to determine whether, as a result of continuous monitoring, (1) the authorizing official is kept sufficiently informed about the operational status and effectiveness of security controls, and (2) the agency promptly mitigates any identified control deficiencies. We also sought to determine whether BIS has resolved the C&A deficiencies we identified in our FY 2006 FISMA evaluation.

To evaluate BIS' continuous monitoring efforts, we interviewed BIS staff to determine what continuous monitoring activity had been performed and to gain further insight on the extent of the security control monitoring. We requested security control monitoring results and evidence; however, BIS was unable to provide any. We also requested an updated system security plan and POA&M to determine if continuous monitoring reporting was adequately performed, but BIS indicated neither had been updated.

In addition, we performed our own assessments of a selected set of security controls (see appendix B) on a targeted set of IT components. We conducted our assessment using a subset of procedures from NIST SP 800-53A, which we tailored to BI's specific control implementations. We did not attempt to perform a complete assessment of each control; instead we chose to focus on specific technical and operational elements. We assessed controls on key classes of IT components, choosing a targeted set of components from each class that would represent the type of components implemented in the system. We also assessed control implementations on [REDACTED] as well as [REDACTED]. In addition, we examined the security plan descriptions, including related policy documents, and interviewed appropriate BIS personnel.

Our assessments included the following activities:

- extraction, examination, and verification of system configurations
- generation of system events and examination of system logs
- execution of the automated vulnerability scanning tool Nessus
- execution of Defense Information Systems Agency (DISA) scripts to assess secure configuration settings for IT products
- addition, modification, and deletion of accounts

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification for a [REDACTED] system would require. However, our assessments gave us direct assurance of the status of select aspects of important system controls.

We used the following review criteria:

- Federal Information Security Management Act of 2002 (FISMA)
- U.S. Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005
- NIST Federal Information Processing Standards (FIPS)
 - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
 - Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
 - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
 - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
 - 800-53, *Recommended Security Controls for Federal Information Systems*
 - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
 - 800-70, *Security Configuration Checklists Program for IT Products*
 - 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* (revised January 2005) issued by the President's Council on Integrity and Efficiency.

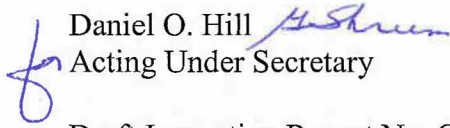
Appendix B: NIST SP 800-53 Security Controls Assessed by OIG

- Account Management (AC-2)
- Access Enforcement (AC-3)
- Least Privilege (AC-6)
- Unsuccessful Login Attempts (AC-7)
- System Use Notification (AC-8)
- Session Lock (AC-11)
- Auditable Events (AU-2)
- Audit Monitoring, Analysis, and Reporting (AU-6)
- Time Stamps (AU-8)
- Protection of Audit Information (AU-9)
- Audit Record Retention (AU-11)
- Configuration Settings (CM-6)
- Least Functionality (CM-7)
- User Identification and Authentication (IA-2)
- Device Identification and Authentication (IA-3)
- Authenticator Management (IA-5)
- Rules of Behavior (PL-4)
- Flaw Remediation (SI-2)
- Malicious Code Protection (SI-3)



SEP 25 2009

MEMORANDUM FOR ALLEN CRAWLEY
Assistant Inspector General
for Systems Acquisition and IT Security

FROM: Daniel O. Hill 
Acting Under Secretary

SUBJECT: Draft Inspection Report No. OSE-195754: *FY 2009*
FISMA Assessment of BIS IT Infrastructure (BI) (BIS002)

Thank you for the opportunity to comment on the above-referenced draft OIG Report. As we discussed prior to the entrance conference for this inspection, the improvement of the Bureau's infrastructure and enterprise architecture is and remains a high priority. The findings and recommendations from the draft OIG Inspection Report have been reviewed and BIS does not dispute the findings.

To ensure compliance moving forward, BIS will produce an action plan to not only address the OIG recommendations for BI but include those recommendations into the operation, monitoring and maintenance of the new infrastructure. As we also discussed previously, recent budget constraints and competing priorities for limited resources have impeded compliance with critical aspects of certification and accreditation. However, I want to assure the OIG that the requirements have been identified and the FY 2010 President's Request will provide the resources needed to replace the BIS IT Infrastructure (BI002) with a more secure infrastructure. The implementation of the new Compartmentalized Application Infrastructure will enable the Bureau to follow the Department's IT security policy and NIST requirements.

If you have any questions comments on our response, please contact Eddie Donnell, BIS' Acting Chief Information Officer, at (202) 482-4296.

cc: Suzanne Hilding
DOC Chief Information Officer

